Cryptocurrencies, Bitcoin and Blockchain: An Educational Piece on How They Work

Mark Keenan
Managing Director, Global Commodities Strategist and Head of Research for Asia Pacific, Société Générale Corporate & Investment Bank (Singapore); and Editorial Advisory Board Member, *Global Commodities Applied Research Digest*

Michael Haigh, Ph.D.
Managing Director and Global Head of Commodities Research, Société Générale (U.S.)

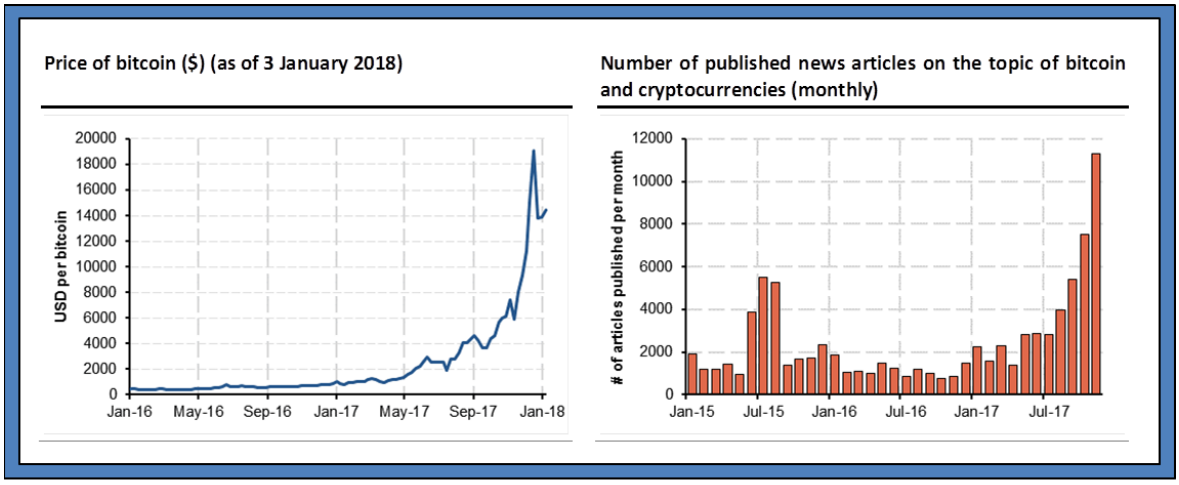
David Schenck
Commodities Analyst, Société Générale (U.K.)

Klaus Baader
Global Chief Economist, Société Générale (U.K.)

Introduction

The market and public curiosity for bitcoin and other cryptocurrencies has been undeniable. Every week, new cryptocurrencies, coins and tokens appear on online exchanges. The exchanges themselves have surpassed, in terms of users, some of the most established traditional stock-broker platforms. For example, it has been reported that Coinbase, a San Francisco-based cryptocurrency exchange, had amassed over 13 million users, some 3 million more than U.S. broker Charles Schwab. If anything, people are paying attention: the number of news articles on the topic of bitcoin and cryptocurrencies has risen substantially; please see Figure 1.

Figure 1



Sources: The Bloomberg, Cryptocompare, SG Cross Asset Research/Commodities.

The articles in this Special Feature do not necessarily represent the views of the JPMCC, its sponsors, or donors.

Needless to say, the nascent sector has attracted a lot of skepticism and criticism. Last year Robert Shiller, a Nobel laureate, said "dabbling in bitcoin lies somewhere between gambling and investing" while former Fed chairman Alan Greenspan said bitcoin was "not a rational currency." Meanwhile, the vice-president of the European Commission, Valdis Dombrovskis, warned E.U. authorities of the "pricing bubble" in the growing cryptocurrency market, and amidst the ongoing chorus of critical comments from central bankers, several bank executives have said bitcoin resembles a scam. Since the significant move higher for most of last year, the digital currency has seen a severe correction.

The sector is still in its infancy and attempting to provide valuations, trade recommendations or any form of investment or trading advice in any capacity is not our objective in this article. Instead, we seek to address the many questions that investors and analysts ask about the nascent technology: what is a bitcoin? What is a blockchain? What problems do these solve? How do decentralized blockchains operate with no central organization? How secure is the blockchain? And what are the limitations embedded in the system? As such, this article is solely educational in nature.

To answer these questions, we structure this paper into three parts.

- In the first part, we briefly describe the nascent cryptocurrency market, focusing on the bitcoin system.

- In the second part, we examine bitcoin's price behavior from a quantitative perspective, highlighting the low correlation of bitcoin and other cryptocurrencies to other traditional asset classes.

- The final section provides a complete overview, including definitions and explanations of all the processes and mechanics behind bitcoin and the blockchain.

PART 1: CRYPTOCURRENCIES – THE NOISE AND THE SIGNAL

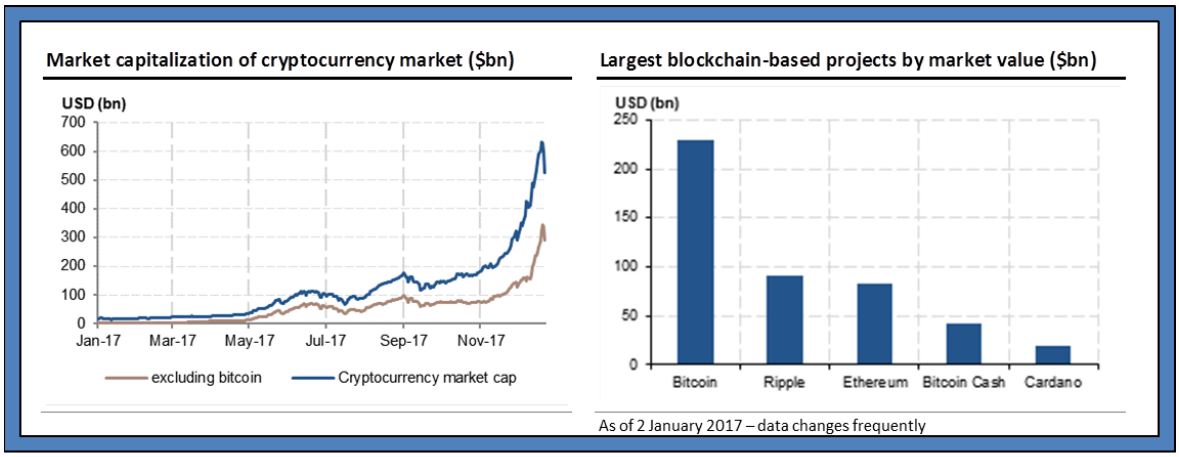
The rise (and fall) of bitcoin prices is reminiscent of previous bubbles: the tulip bubble of 1637 in terms of prices, and more recently, the internet bubble in the late 1990s. Evidence is growing that the cryptocurrency craze was spilling over to other asset classes. For example, when Long Island Iced Tea Corp. (LTEA US Equity) rebranded to Long Blockchain Corp. in late December 2017, investors flocked to buy the company's stock, driving a 200% price increase overnight.

The cryptocurrency market may be in a bubble and valuations may be out of control, but the technology known as blockchain, underlying bitcoin and other cryptocurrencies, is likely here to stay. In spite of the valuation excesses and noise, the aggregate market capitalization of the cryptocurrency market, having breached $700bn, suggests we may have already potentially sowed the seeds of a new asset class.

According to Coinmarketcap, dollar-valuations of the money supply (i.e., market cap) in the form of cryptocurrency rose 40-fold in 2017, rising from $15bn to $640bn. Bitcoin is perhaps the sector's most prominent example, but other coins are competing for dominance. (Please see Figure 2 on the next page.) Bitcoin's market share of the cryptocurrency market has already fallen below 40%, and over 1,350 blockchain-based projects already have exchange-traded tokens.[1]

Within the cryptocurrency sector, it is perhaps worthwhile to distinguish coins intended to replace traditional fiat currency from tokens, used in smart-contract blockchains and for which convertibility into fiat money is almost secondary.[2] Bitcoin and its spin-offs (such as Bitcoin Cash and Bitcoin Gold) have no other intended purpose than as a medium of exchange. In contrast, Ethereum coins (ETH) and its underlying blockchain, were designed to execute smart contracts, and the convertibility of these coins into fiat money (e.g., USD) is a secondary, albeit necessary condition for the operation and maintenance of the blockchain.

Figure 2



Sources: Coinmarketcap, SG Cross Asset Research/Commodities.

Unlike bitcoin, many blockchain-based projects are led by centralized organizations – often in the form of non-profit organizations (e.g., Ethereum Foundation), but also in the form of for-profit corporations (e.g., EOS's Block.one Corp.). According to Coinschedule, over 200 blockchain-based projects have successfully completed initial coin offerings (ICOs) in 2017, raising nearly $3.6bn from private investors. The proceeds of these ICOs are often earmarked for funding research and development in the underlying infrastructure (e.g., software development.) Among the notable 2017 ICOs, we recall Filecoin's ($257m) in August 2017, Tezos' controversial $232m as well as EOS' $185m fundraising.

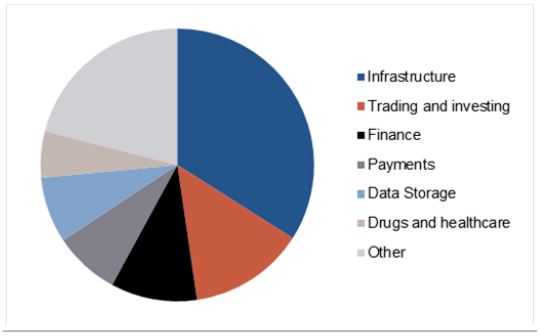
As shown in Figure 3 on the next page, many of these projects are based on payments and financial applications, but a sizeable fraction of the market is nevertheless focused on delivering infrastructure and data-storage solutions.

Figure 3

Ten largest 2017 initial coin offerings (ICO)

Company	Funds raised during ICO
Filecoin	$ 257 000 000
Tezos	$ 232 319 985
EOS Stage 1	$ 185 000 000
Paragon	$ 183 157 275
Bancor	$ 153 000 000
Kin Kik	$ 97 041 936
Status	$ 90 000 000
TenX	$ 64 000 000
MobileGO	$ 53 069 235
KyberNetwork	$ 48 000 000

2017 ICOs by category (weighted by funds raised)



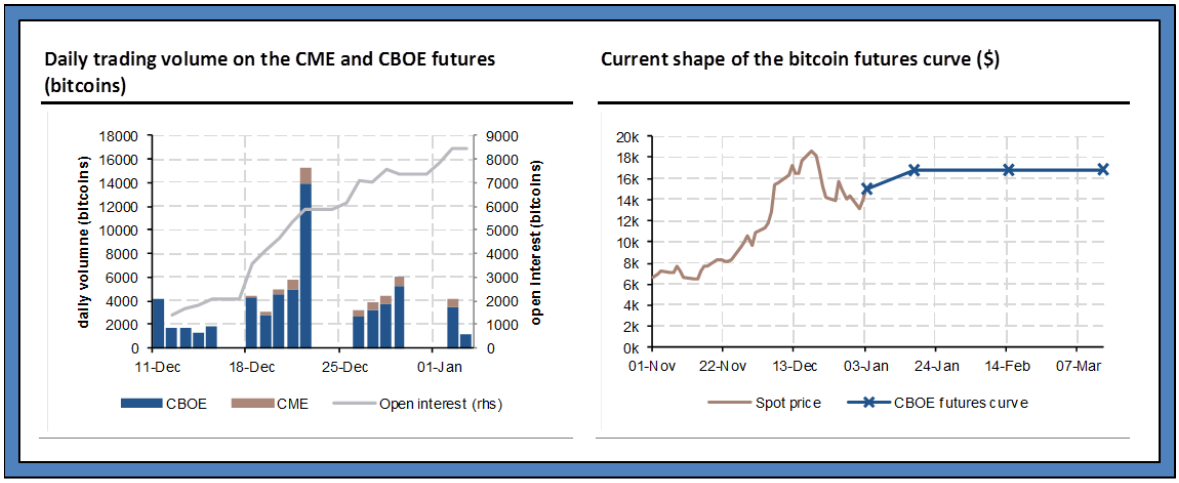
Sources: SG Cross Asset Research/Commodities, Coinschedule.com.

The Proliferation of Bitcoin Related Products

In practice, participation in ICOs is still limited to venture capitalists and retail investors lured by short-term returns, but cryptocurrencies look likely to find ways to encroach into traditional finance in the near term. The low interest-rate environment has also perhaps boosted the growth of the sector, increasing the relative appeal of alternatives to traditional money and, as long as we are in a very low rate world, the fashion for cryptocurrencies and tokens could continue. Bitcoin still trades very much on the fringe of mainstream finance, but it has a foot in the door. Some players have already seized the opportunity: assets under management with the Bitcoin Investment Trust ETF (GBTC US Equity) have, for example, grown to above $2bn, up from $160m a year earlier, and the CME and CBOE have launched cash-settled futures on bitcoin.

At the end of 2017, the volumes on both these exchanges started out relatively light; please see Figure 4 on the next page.

Figure 4



Sources: Bloomberg, SG Cross Asset Research/Commodities.

On CBOE futures, the reportable position level is set at five contracts, equivalent to a long or short futures exposure of five bitcoins. Traders holding positions in excess of this limit must currently disclose their positions to the Commodity Futures Trading Commission (CFTC), which then reports the aggregate position on a weekly basis in their weekly Commitments of Traders (COT) report. The table on the left-hand side of Figure 5 on the next page reports the data as of December 26, 2017. At the time, there were no commercial traders involved in the futures market. 34 non-commercial traders (i.e., large speculators) were net short of 1,801 contracts. By construction, small traders held the remaining long open interest.

The data were too thin to identify trends and characterize market structure, but we found the initial breakdown intuitive: the futures markets served primarily as a venue for shorting the cryptocurrency. Longer term, commercial traders could appear in the form of bitcoin miners, who validate transactions on the network, and look to hedge their fiat-denominated costs (e.g., electricity, hardware) with bitcoin revenues.

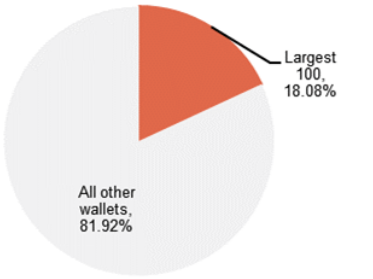
Perhaps a more telling (and daunting view) of the bitcoin market involves looking at the holding concentration of the largest wallets (akin to accounts.) Since all bitcoin transactions are public, it is possible to compute the balance of each wallet on the network. According to Bitinfocharts, the largest 100 wallets hold approximately 18% of all bitcoins. (Please see the pie-slice chart on the right-hand side of Figure 5 on the next page.) It also estimates that there are at least 2,442 wallets holding bitcoins worth more than $10m each. On the one hand, this figure may overstate concentration, as some of these wallets are exchange vaults holding client deposits. On the other hand, this breakdown may underestimate concentration, as anyone on the network can create as many wallets as he or she wishes.

Figure 5

CFTC Commitment of Traders report on CBOE bitcoin futures, week of 26 December

Non-commercial	
Long	1232
Short	3033
Spreading	117
Net position	*-1801*
Non-reportables	
Long	2388
Short	587
Net position	*1801*
Total	
Open interest	*3737*

Largest 100 wallets hold 18% of all bitcoins

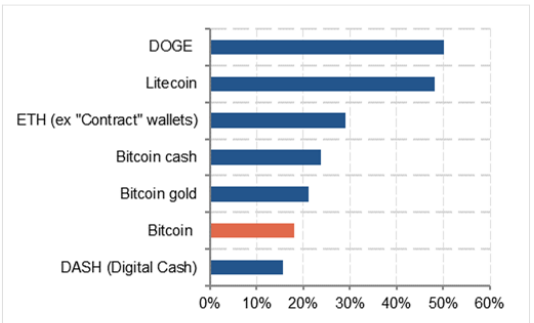


Sources: SG Cross Asset Research/Commodities, CFTC, Bitinfocharts.

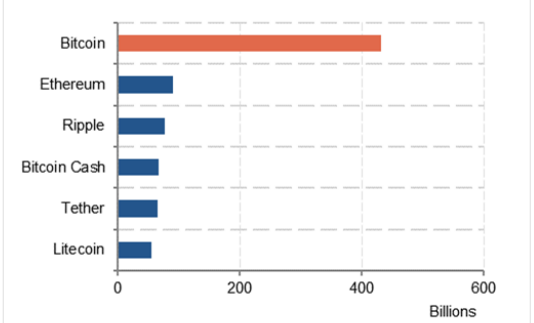
On other blockchains, concentration is equally problematic: according to Etherscan, the largest 100 Ethereum wallets (excluding "Contract" wallets, which are "smart contract" accounts not held by individual holders) currently hold 29% of all issued coins. On the Litecoin blockchain, the largest 100 wallets control over 48% of the coin supply; please see the bar chart on the left-hand side of Figure 6. And on the DASH blockchain, the largest 100 wallets concentrate 16% of the circulating supply. Again, these figures may overestimate concentration since some wallets may refer to exchange vaults aggregating client deposits, but clients can conversely create many wallets at no additional cost.

Figure 6

Supply held by largest 100 wallets, for selected blockchains



30-day observable trading volume for largest six coins ($bn)



Source: SG Cross Asset Research/Commodities.

In terms of exchange trading volume, bitcoin has dominated the cryptocurrency space, as shown in the bar chart on the right-hand side of Figure 6.

Defining Cryptocurrencies

Are cryptocurrencies, like bitcoin – and as their name suggests – actual currencies? Or should we treat them as commodities? Considering the basic definition of money (unit of account, means of transaction, store of value), it is understandable why the jury is still very much out on the subject, and we currently see the nascent sector having many features like commodities. Like gold, the value of bitcoin is primarily socially determined. Both gold and bitcoins are divisible and fungible. While the supply of gold is assumed to be finite, the maximum supply of bitcoin is set at 21 million. As no government (currently) recognizes bitcoin or other cryptocurrencies as legal tender, it therefore perhaps makes more sense for bitcoin to be classified as a commodity rather than as a fiat currency.

The question is not purely academic either, as the way national governments and regulators decide to treat cryptocurrencies will determine and shape how/whether the sector develops and evolves.

- The CFTC said it considered tokens issued through initial coin offerings to behave as commodities. In a September 2017 ruling against a San Francisco-based start-up, the CFTC decided that bitcoin and other digital cryptocurrencies were covered by the Commodity Exchange Act (CEA).

- The Securities Exchange Committee (SEC) has already stopped several ICOs, in effect ruling that cryptocurrencies and digital tokens fell within its mandate. The SEC has also refused to approve several cryptocurrency-based ETFs, and warned investors against scams.

- The U.S. Internal Revenue Services (IRS) says bitcoin must be treated as intangible property. Capital gains and losses must be reported for tax purposes.

- The U.S. Treasury has said "virtual currency does not have legal tender status in any jurisdiction."

Outside of the U.S., official organizations have also issued rulings. For example:

- In China, financial institutions are banned from accepting, using or selling virtual currencies. Exchanges must register with the government.

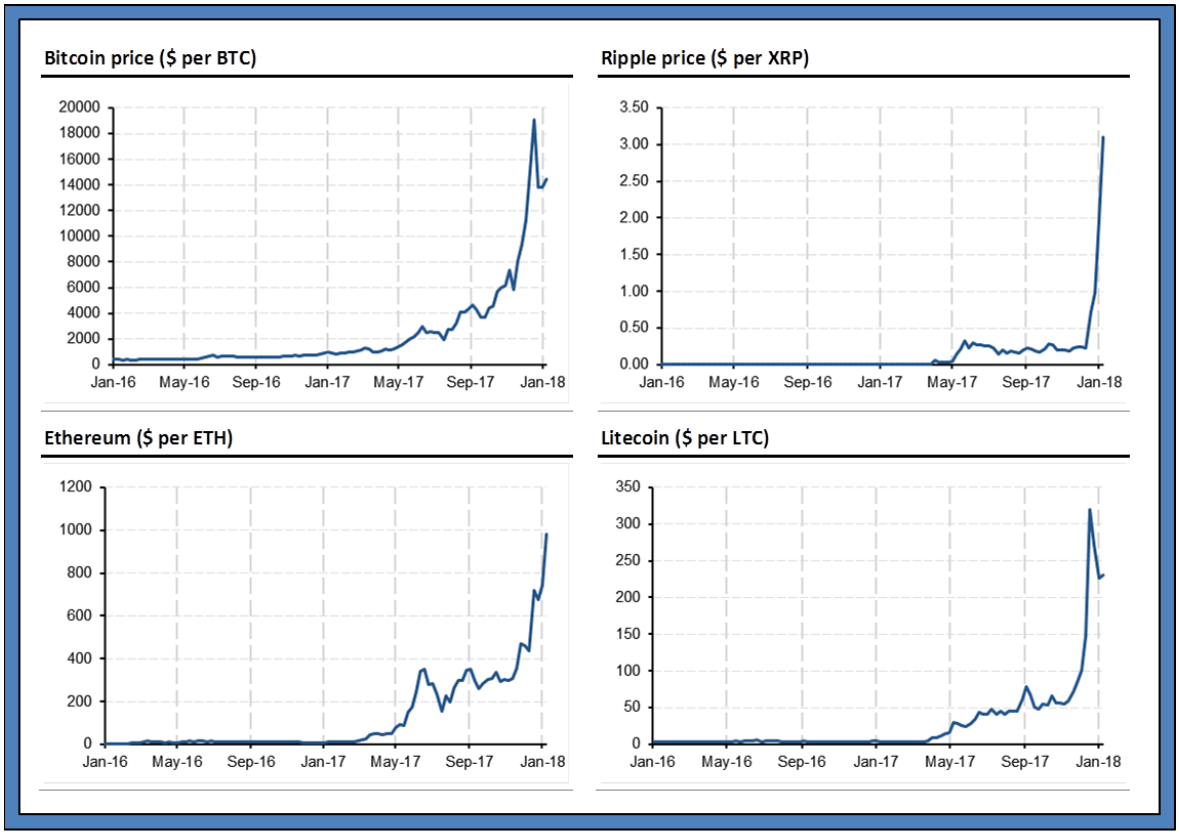
- In a ruling against one of its member states, the European Central Bank has banned E.U. members from introducing government-backed digital currencies.

- In Egypt, the Grand Mufti has issued a fatwa (religious ruling) against the use of bitcoin.

PART 2: FINANCIAL SPECS OF CRYPTOCURRENCIES AND RETURN VERTIGO

The return on cryptocurrencies had been spectacular, if not surreal, as illustrated in Figure 7 on the next page.

Figure 7

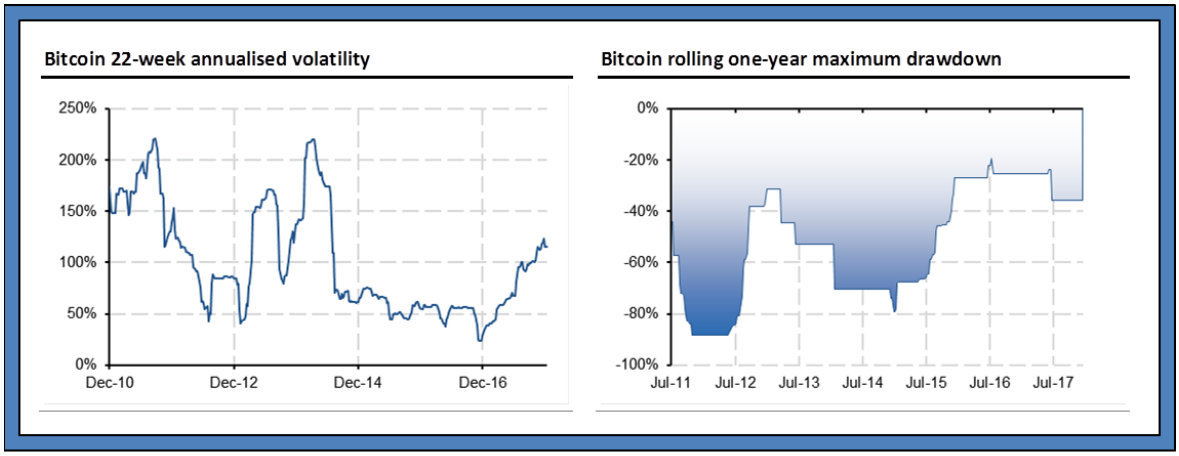


Sources: CryptoCompare, SG Cross Asset Research/Commodities.

Extreme Volatility

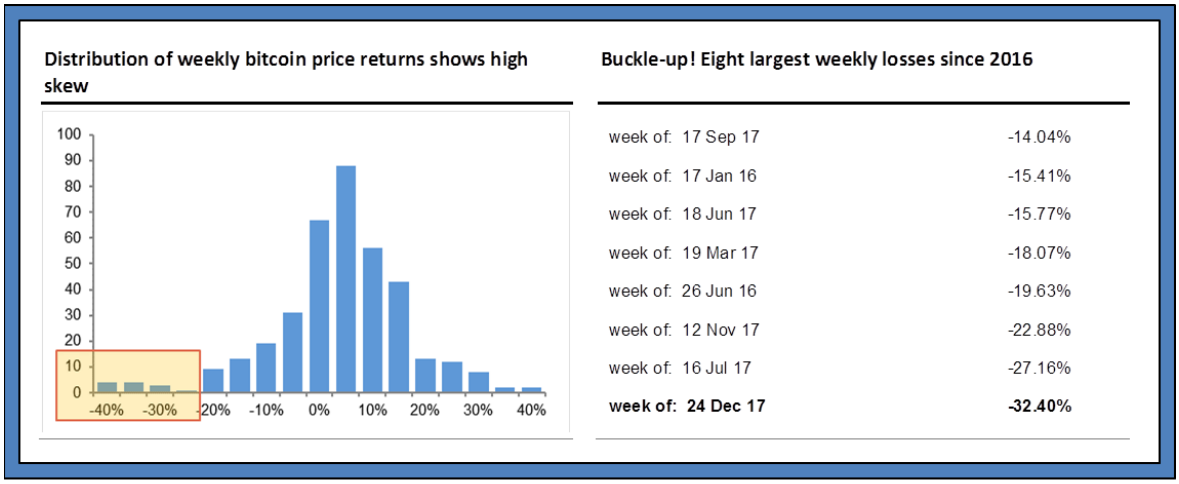
For instruments intended to replace fiat currency, bitcoin and other cryptocurrencies have scored poorly on the "store of value" criteria, given their bouts of extreme volatility. Figure 8 on the next page illustrates bitcoin's past high volatility and maximum drawdown figures while Figure 9, also on the next page, shows how highly skewed bitcoin's returns have been along with the scale of its past large weekly losses.

Figure 8



Source: SG Cross Asset Research/Commodities.

Figure 9

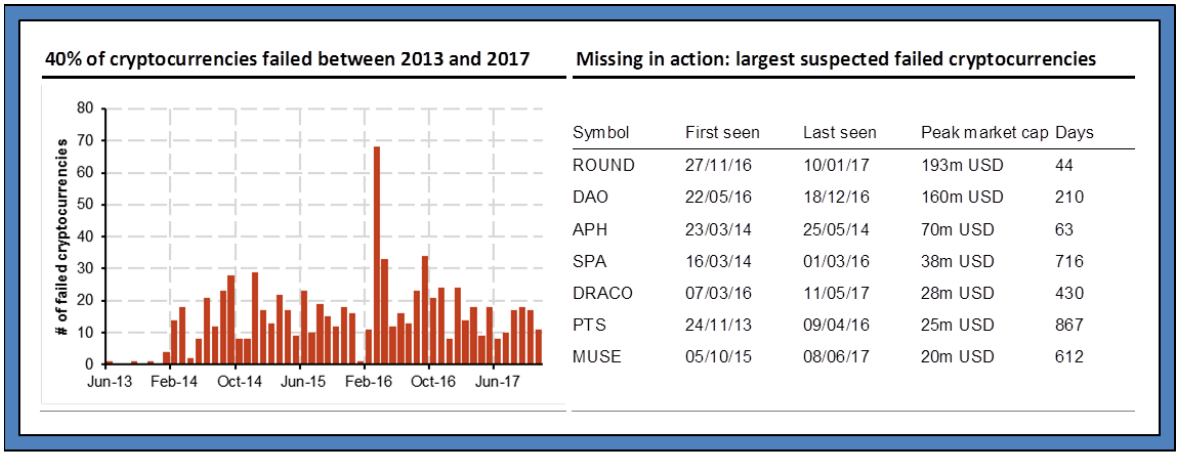


Source: SG Cross Asset Research/Commodities.

Survival Bias

Besides the past high levels of volatility, the survival rate of cryptocurrencies is rather low. Using data provided by Coinmarketcap going back to April 2013, we found more than 860 defunct cryptocurrencies, representing 40% of the observable universe of cryptocurrencies; please see Figure 10 on the next page. Furthermore, it is not unlikely that many more cryptocurrencies failed to launch after their initial coin offering – suggesting that these statistics are probably conservative. As of the writing of this article, the average lifetime of defunct cryptocurrencies stands at 327 days, compared with 513 days for surviving cryptocurrencies. There was a notable surge of cryptocurrency extinctions in March 2016, when the price of bitcoin fell by over 25%.

Figure 10



Missing in action: largest suspected failed cryptocurrencies

Symbol	First seen	Last seen	Peak market cap	Days
ROUND	27/11/16	10/01/17	193m USD	44
DAO	22/05/16	18/12/16	160m USD	210
APH	23/03/14	25/05/14	70m USD	63
SPA	16/03/14	01/03/16	38m USD	716
DRACO	07/03/16	11/05/17	28m USD	430
PTS	24/11/13	09/04/16	25m USD	867
MUSE	05/10/15	08/06/17	20m USD	612

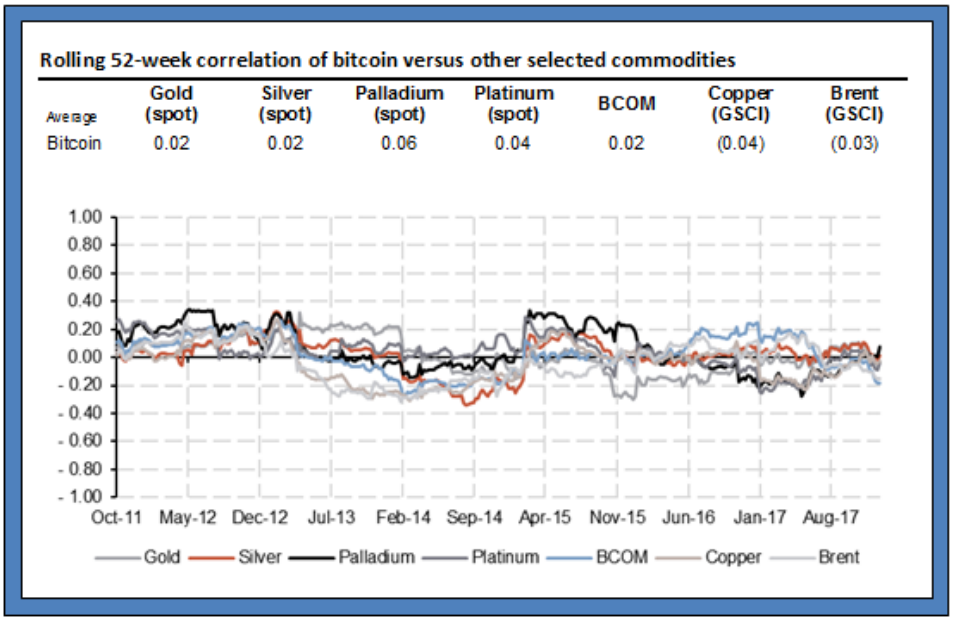
Source: SG Cross Asset Research/Commodities.

The above right-hand table of Figure 10 further shows the largest seven suspected failed cryptocurrencies. At their price peak, the dollar value of the circulating supply was worth tens and in some cases hundreds of million dollars. ROUND and DAO coins were worth, in aggregate, $193m and $160m at their market peak. Going forward, it is likely that the high rate of failure will persist, or perhaps even increase as more new products appear.

Correlation Profiles

We computed the correlation of bitcoin weekly returns against the return of several financial instruments across several asset classes, and not surprisingly found they are unrelated, as the price behavior of bitcoin has been entirely speculative. For the period from July 2010 to January 2018, the weekly return correlation of bitcoin with commodities hovered near zero; please see Figure 11 on the next page.

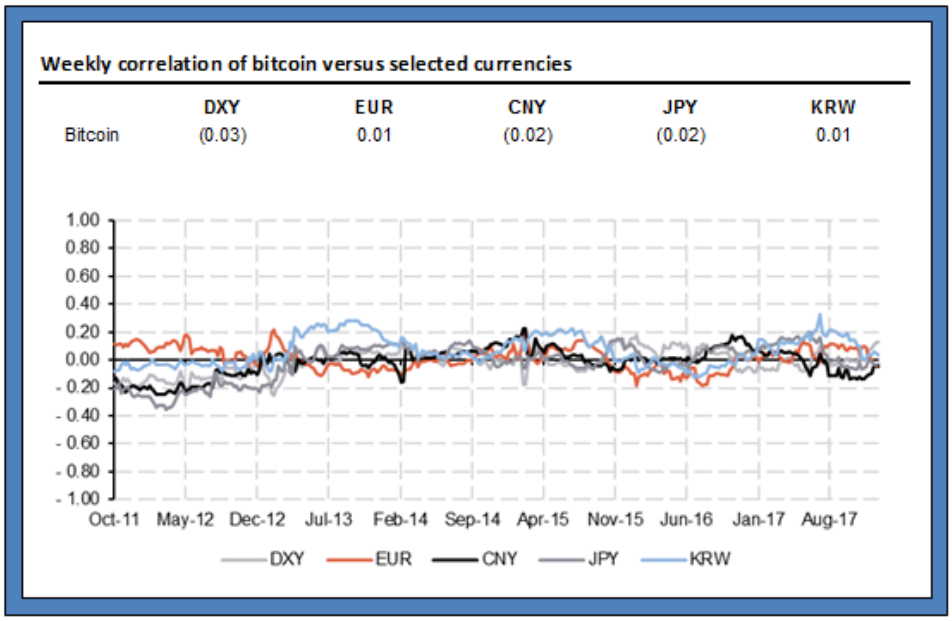
Figure 11



Source: SG Cross Asset Research/Commodities.

Likewise, correlations with selected fiat currencies revealed no relationship, as shown in Figure 12.

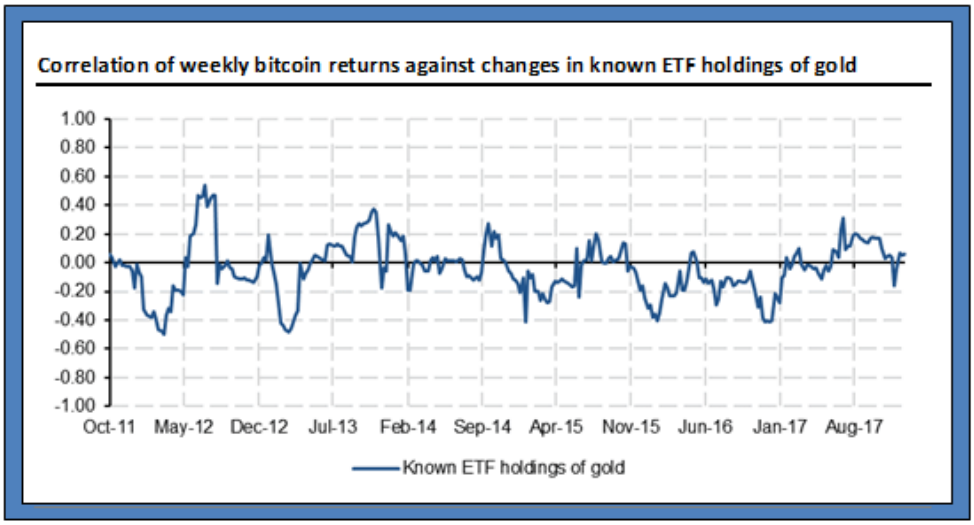
Figure 12



Source: SG Cross Asset Research/Commodities.

We computed the rolling six-month correlation between weekly bitcoin returns and changes in known ETF holdings of gold (ETFGTOTL Index) to assess whether there might be a relationship between flows into gold ETFs and bitcoin prices. Here also, we found little relationship, as seen in Figure 13.

Figure 13



Source: SG Cross Asset Research/Commodities.

Finally, we also computed the cross-correlation of weekly returns between some of the largest or most established cryptocurrencies, as shown in Figure 14. Interestingly, we found that cryptocurrencies themselves exhibit low levels of cross-correlation. This underscores the extreme level of speculation and the absence of any meaningful structure, relationship or cohesion amongst the cryptocurrencies in our analysis. The highest recorded level of correlation was found to be with Litecoin (LTC), at 0.40.

Figure 14

Weekly return correlations

	ETC	XMR	MIOTA	XLM	LTC	XEM	DASH	ETH	BCH	XRP	BTC
ETC	1.00	0.05	0.01	0.06	0.09	0.06	0.03	0.10	-0.01	0.02	0.05
XMR		1.00	0.06	0.08	0.14	0.12	0.11	0.10	0.03	0.01	0.14
MIOTA			1.00	0.17	0.05	0.09	0.09	0.10	0.06	0.00	0.14
XLM				1.00	0.13	0.19	0.11	0.08	0.00	0.31	0.10
LTC					1.00	0.20	0.11	0.07	0.03	0.18	0.40
XEM						1.00	0.05	0.14	0.03	0.11	0.11
DASH							1.00	0.10	0.07	0.00	0.17
ETH								1.00	-0.01	0.05	0.11
BCH									1.00	-0.01	0.00
XRP										1.00	0.14
BTC											1.00

Source: SG Cross Asset Research/Commodities.

PART 3: UNTANGLING BITCOIN AND THE BLOCKCHAINS

Cryptocurrencies as a concept is still relatively new, and investors are keen to understand the new technology to assess potential value, if any. In this section, we therefore define bitcoin and its underlying blockchain. To shed light on some of the system's trickiest details, we provide a rudimentary overview of the cryptographic principles underlying blockchains.

What is Bitcoin?

A bitcoin simultaneously refers to a unit of account as well as a decentralized system of payment. In its foundational paper, published in 2007, Satoshi Nakamoto, its pseudonymous author, described the system as a pure "peer-to-peer version of electronic cash," allowing participants to transfer online payments directly from one to another without the need for a centralized financial institution.

Multiple projects have attempted to create a decentralized virtual currency as early as the 1990s. However, the first practical implementation of bitcoin only appeared in 2009 with the release of the bitcoin software. Bitcoin's first transaction (the genesis block) contains, as a comment in its metadata, "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", a reference to the headline of the front-page of the British newspaper, *The Times*, published early in 2009. The first recorded bitcoin-based transaction famously dates to May 2010 when a Florida-based user of the online bitcointalk.org forum successfully traded 10,000 bitcoins with another user in exchange for two pizzas at a local vendor.

Since then, bitcoin has evolved and grown to become the world's largest digital currency by market capitalization. As we noted in the first section, bitcoin related products have started to emerge (ETFs and futures), crossing into more mainstream financial channels, but despite this, its extreme volatility and the numerous questions on its innate viability combined with uncertainty surrounding its longevity remain considerable.

One particular feature of bitcoin is its limited supply, capped at 21 million units. Each bitcoin is also divisible into 1 million individual parts commonly known as *satochis* in reference to the anonymous author of the original paper.

What Problem Does Bitcoin Intend to Solve?

As described by its author, bitcoin intends to become "peer-to-peer electronic cash." It aims to allow the online ("electronic") transfer of value from one participant to another ("peer-to-peer") without the need of a centralized organization such as a clearing house or a bank (instead relying on decentralized ledgers.)

In its foundation paper, Satoshi Nakamoto explained that "commerce on the internet has come to rely exclusively on financial institutions serving as trusted third parties to process electronic payments." According to the author, this system, based on "trust," has "inherent weaknesses" in the form of high transaction costs, fraud, and mediation. Importantly, and unlike physical currency, online transactions

are "reversible" and "merchants must be wary of their customers, hassling them for more information than they would otherwise need."

As it currently stands, electronic commerce indeed relies heavily on centralized organizations such as PayPal, VISA, MasterCard and banks to enforce and secure online payments and transfers. In exchange for the trust they provide, these organizations charge a processing fee, often in excess of 1% of the value. Businesses providing remittances services (e.g., Western Union) similarly charge significant fees to transfer value from one part of the planet to another.

Bitcoin intends to substitute the trust-based model involving intermediaries with a payments system based on cryptographic proof, "allowing two willing parties to transact directly with each other without the need for a trusted third party."

Where is the Money?

Bitcoin, like other currencies (e.g., the euro, U.S. dollar) has no intrinsic value other than the social value we agree on. We accept to make transactions in bitcoins just the way we accept to make transactions in U.S. dollars – with the assumption that we can later use the proceeds to make further purchases and believing that others will do the same.

However, unlike hard currency or even intangible commodities like electricity, a bitcoin has no physical form besides a seemingly-random string of characters recorded on the system. Moreover, this string of characters is publicly visible to all participants in the bitcoin network, and its source is also perfectly traceable.

Ownership, therefore, takes the form of a social construct and is distinct from physical possession. To understand bitcoin, it is best to compare it with intellectual property: bitcoin ownership exists much the way patents and copyrights only exist within the legal framework in which these were designed and granted. Neither bitcoin nor patents have physical substance besides the written social contract in their respective systems.

Each bitcoin in circulation is, at any time, associated with an address, as shown in the image above. An address is a string of characters and uniquely identifies a bitcoin wallet, much the way an IBAN (international bank account number) uniquely defines a bank account number. Each wallet also has a password-like secret key. Anyone in possession of the secret key can use the wallet and move funds out.

How are Bitcoins Acquired?

To acquire bitcoins, one needs to find another participant willing to sell. To improve liquidity, buyers and sellers often meet on digital exchanges, but one could just as well find someone on the street and exchange directly with him provided a mutually-agreed price can be found. The seller needs to send the bitcoins to your public address in exchange for which you provide dollars, euros, goods or services.

The Issue of Trust

To keep track of each user's balance, the bitcoin system keeps a history of transactions, known as the blockchain. The blockchain is a file containing the history of all transactions on the bitcoin network. Unlike hard currencies like the U.S. dollar, bitcoin and other cryptocurrencies operate without a central organization such as a commercial bank, a clearing house, a central bank or a government. Instead, the source of truth and ultimately people's faith in the currency lies with the blockchain itself, which is distributed and decentralized among the network participants. Distribution refers to the idea that many participants simultaneously own parallel copies of the blockchain while decentralization refers to the notion that changes to the blockchain are ultimately decided by the majority of participants through a process known as consensus.

To claim ownership over a bitcoin, one has to demonstrate having received the bitcoin in a previous transaction – and the blockchain (or history of transactions) serves as the "paper trace" of these transactions. As such, ownership is enforced not by any single party or judge, but rather by consensus among the participants on the bitcoin network, all of whom simultaneously maintain a copy of the ledger.

Figure 15

Block #	Timestamp	Transactions	Recorded by	Size
502343	Jan 3, 2018 10:28:30 AM	2472		983392
502342	Jan 3, 2018 10:21:01 AM	2348		962408
502341	Jan 3, 2018 10:17:41 AM	1913	AntMiner	979423
502340	Jan 3, 2018 9:23:08 AM	2684	AntMiner	948962
502339	Jan 3, 2018 9:21:13 AM	2553	AntMiner	973348
502338	Jan 3, 2018 9:17:57 AM	2571	AntMiner	978949
502337	Jan 3, 2018 9:08:27 AM	2796	AntMiner	972043
502336	Jan 3, 2018 8:54:17 AM	2644		968652

Sources: SG Cross Asset Research/Commodities, Blockexplorer.com.

For efficiency purposes, the bitcoin blockchain records transactions in groups called blocks. The above table in Figure 15 shows the most recent eight blocks recorded on the blockchain during one timeframe. The most recent block (block #502343) was recorded on 3 January 2018 at 10:28am and contained 2,472 individual transactions. One of these transactions is shown in Figure 16 on the next page and involves the transfer of 0.076 bitcoins from one address to another.

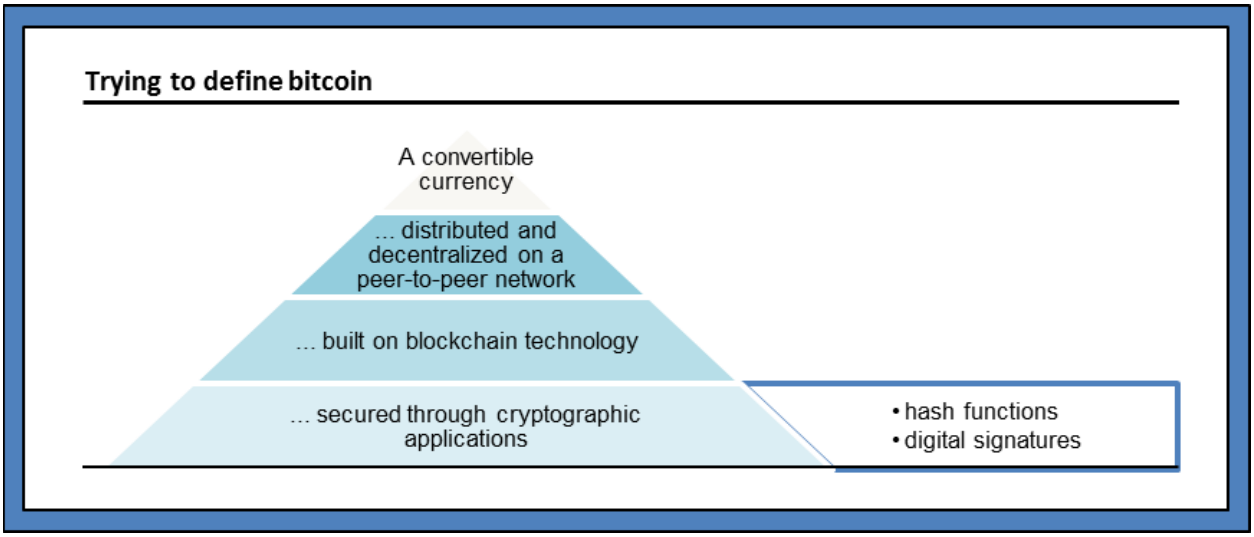
Figure 16

Sources: SG Cross Asset Research/Commodities, Blockexplorer.com.

The Bitcoin Invisible Hand

The decentralized nature of bitcoin is a key feature of the system, and understanding how the blockchain operates with no centralized organization is fundamental in any attempt to understand the digital currency. We illustrate bitcoin's fundamental design in Figure 17.

Figure 17



Source: SG Cross Asset Research/Commodities.

At the lowest level, bitcoin is based on a few cryptographic concepts such as hash functions and digital signatures. These jointly provide security and authentication. As explained above, transactions are recorded in a file-like ledger known as the blockchain. Unlike traditional ledgers, blockchains are immutable, meaning that past transactions can neither be altered nor reversed. The blockchain itself is distributed and decentralized on the bitcoin peer-to-peer network such that no single party controls the blockchain. Faith in the currency's security and decentralization then allows the virtual currency to achieve convertibility into other fiat currencies. We review each of these layers in turn.

Layer 1: Cryptographic Foundation

At its core, the existence of bitcoin and other blockchains is predicated on a set of cryptographic concepts, which allow these systems to operate in decentralized but nevertheless coordinated manners. While these concepts are mathematically very complex, a principle understanding of these concepts allows for a better understanding of the way blockchains ultimately achieve what they are designed to do – namely, maintaining an immutable ledger of transactions.

We therefore begin by introducing hash functions, one of the protocol's basic building bricks, the understanding of which will allow us to then better comprehend hash puzzles and bitcoin mining. We also briefly introduce digital signatures that underpin authentication and authorization in blockchains.

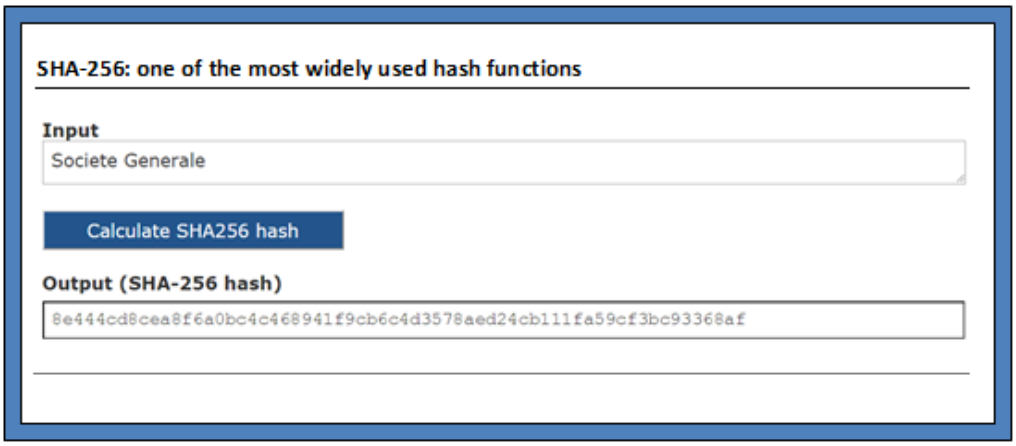
Hash Functions

Blockchains rely heavily on cryptographic algorithms known as hash functions. In computer science, a function is a set of computer instructions (an algorithm) designed to convert an input (e.g., a number, a sequence of characters) into an output.

Hash functions are a group of functions designed to accept a sequence of characters of any length and convert that input into a fixed-length sequence of characters. We say a hash function converts an input into its hashed representation. This representation is known as the hash digest, or just hash.

The most widely-used hash function is known as **SHA-256**, which was designed and open-sourced by the U.S. National Security Agency (NSA) in the early 2000s. This particular hash function maps an arbitrary input to a sequence of 64 characters (encoded by 256 bits.) Although the hash function creates a seemingly random output, the output is nevertheless consistent every time it is performed on the same input. By way of illustration, the hash representation of "Societe Generale" (the input) using the SHA-256 algorithm is represented in Figure 18. As expected, the digest has fixed-length (64 characters.)

Figure 18



Source: SG Cross Asset Research/Commodities.

There are many hash functions, but for these functions to be useful in cryptographic applications, these must have a number of desirable features. Specifically, hash functions must be computationally efficient, minimize collisions, conceal the input message, and must be puzzle-friendly. We briefly explain what each of these features mean:

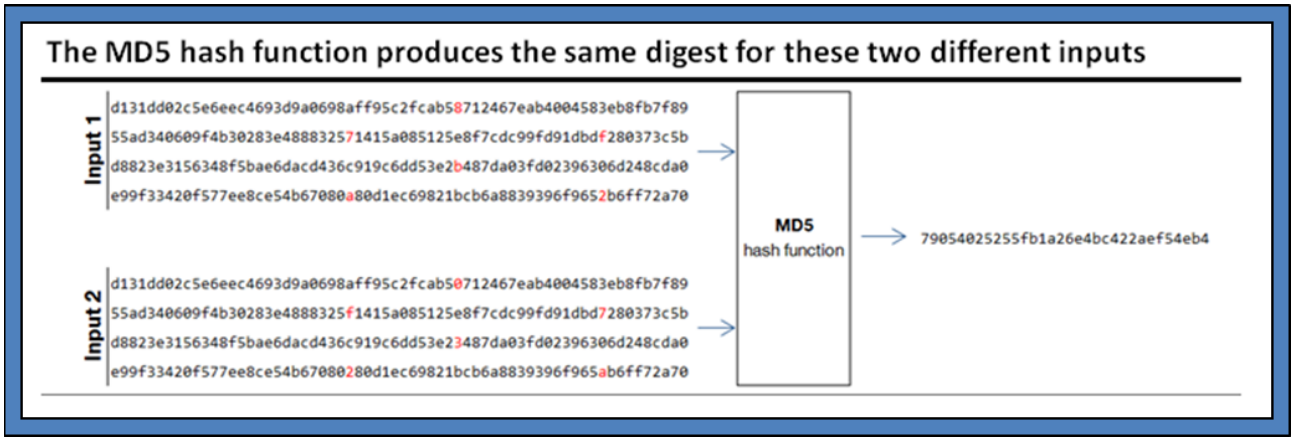
1. Firstly, hash functions should be computationally efficient – meaning that the computation of the hash function for a given input must be technically feasible with the average available hardware. Currently, the average computer or telephone can compute several hundred thousand SHA-256 functions per second – making this algorithm computationally efficient.

2. Furthermore, hash functions should be collision-free. A collision arises when the digest (or hashed representation) of two different inputs are the same.

   Collisions should theoretically be inherent to hash functions since the universe of possible inputs is significantly larger than the universe of possible outputs. We recall that the input to a hash function can be of any size while the output of the hash function has fixed-length. For example, the SHA-256 algorithm always yields 64-character outputs. There is therefore a limited universe of possible outputs, specifically 2^{256} possible outputs – please see the side box on the next page. The number of inputs is, on the other hand, however infinite, implying that collisions are inherent to hash functions.

   For example, MD5, another widely-used hash function was "broken" in 2005 when researchers from Shandong University in China described how two different sequences (shown in Figure 19) produced the same hash (i.e., a collision) when passed to the MD5 hash function.

Figure 19



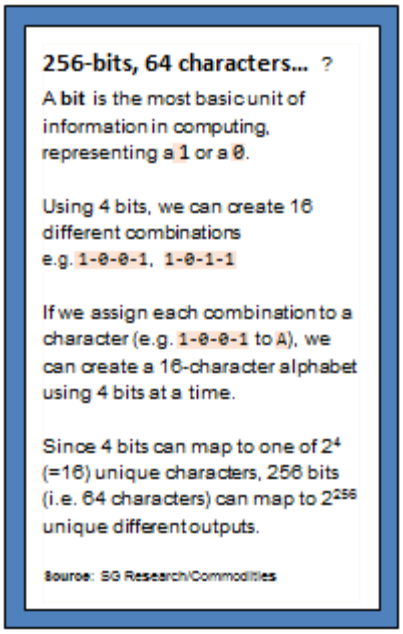
Sources: http://www.mathstat.dal.ca/~selinger/md5collision/, SG Cross Asset Research/Commodities.

Although no hash function can theoretically be collision-free, some hash functions are notably efficient at minimizing them. For example, the SHA-256 algorithm has, to date, not produced a collision. Stated differently, we have thus far been unable to find two different inputs which transform into the same digest when passed to the SHA-256 function.

As it stands, one could try 2^{130} different inputs through the SHA-256 hash function (an unreasonably large number), and then, the probability of finding a collision would still be below 100%.

Collision-free hash functions, like the SHA-256 algorithm, have a number of useful properties. Principally, if the hash function is known to be collision-free, then the digest uniquely represents or identifies the input – there is a (probabilistic) one-to-one mapping of input to output. Stated differently, the hash output is akin to a digital fingerprint of the input. If we see two identical hashes, then it is safe to assume that the inputs are the same. And, because hashes are often shorter than the inputs that they represent, hash functions succinctly and wholly summarize inputs.

3. Hash functions should obfuscate or conceal the original input. Given a digest, it must be difficult to find the original input without further knowledge of the possible universe of inputs – stated differently, it must be difficult to decipher the output of the hash function. Again, the SHA-256 function succeeds at this – there is indeed no easy way to see that underlying the hash 8e44[…]36af is the input "Societe Generale."



4. Hash functions must be puzzle-friendly: given a hash function (e.g., SHA-256) and a subset of outputs, there should be no better way to find an input that converts into one of the outputs than to try randomly. For example, given the SHA-256 algorithm, if we wanted to find an input whose digest started with a "0", there would be no better way than to try random inputs until we indeed found one.

   For example, if one wanted to find the lowest number whose SHA-256 hash started with five zeroes (e.g., "00000691457f…"), there would be no better way than to try numbers until one was found. This number is 596,138.

Ensuring that hash functions are both collision-free and puzzle-friendly may seem like two faces of the same coin, but they ultimately achieve different objectives: the collision-free feature ensures the uniqueness of the input-output mapping: given two identical hashes, the probability that they were produced using the same input converges to 1 for collision-free hash functions. Puzzle-friendliness, on the other hand, ensures the randomness of the algorithm such that to produce a desired pattern, there is no smarter way than to try random inputs.

Digital Signature

Digital signatures are another common cryptographic application and a foundational concept underlying bitcoin and other blockchains. While the mathematical derivation of the concept is beyond the scope of this paper, understanding the mechanism is nevertheless vital for a thorough understanding of the blockchain.

Like a handwritten signature (such as in the right-hand box), a digital signature should fulfil two requirements:

1. Only the signee can append his signature to a document or message – he is the sole owner of the signature, and his signature commits the signee to the content of the message on which he appended his signature;

2. Anyone can verify the authenticity of the signed message by looking at the signature.

In practice, manuscript signatures are not impossible to counterfeit. Digital signatures improve on this and are nearly impossible to counterfeit, provided a number of conditions are fulfilled.

Digital signatures are often implemented using a public-private key algorithm, the most famous of which is known as RSA-encryption. In public-private key encryption, two related-but-different sequences of characters known as keys are first generated:

- The first is known as the public key, and, as the name suggests, can be distributed widely.

- The second key is known as the private or secret key. As the name suggests, the private key must be kept secret and acts as a password.

Importantly, only the public key can decrypt a message encrypted by the private key, and vice versa. Encryption refers to the process of concealing a message such that only the holder of the key can reveal the original message. This asymmetry effectively allows one party to sign a document and another party to authenticate the document. (Digital signatures are contrasted with hash functions in Box 1 on the next page.)

For instance, suppose that Mark wanted to send a signed message to Sophie (e.g., “Mark pays Sophie $20”.) Mark could then encrypt the message using his private key, send the encrypted message as well as his public key to Sophie. Sophie, receiving these two elements, can then decrypt the message using Mark’s public key. A valid decryption not only reveals the message, but simultaneously verifies that the message was indeed encrypted by Mark and is authentic. As a matter of fact, anyone (including Sophie) can verify the message’s authenticity as the public key is … public.

Box 1

Summary: hash functions and digital signature

Hash functions and digital signatures are two key cryptographic concepts underlying blockchain technologies. Although related, hashing and signing are nevertheless different in their **reversibility**: the output of a hash function **cannot** be converted into its original input using a known function. Digital signatures on the other hand are a form of **encryption**: the encrypted output can be reconverted to its original form provided the correct key is provided.

Hashing
one-way

Encryption (e.g. digital signatures)
two-way

Public key encryption plays a central role in bitcoin and other blockchains. As a matter of fact, each account (known as a wallet) is in fact defined by a public key, known as the address. The only person able to move bitcoins out of a wallet is the person who knows the private key associated with the wallet's address. On the bitcoin network therefore, users can create new wallets at will, by creating new public-private key pairs. As a matter of fact, users are encouraged to generate multiple wallets to protect privacy, by distributing their holdings across several wallets; please see Figure 20.

Figure 20

Source: SG Cross Asset Research/Commodities.

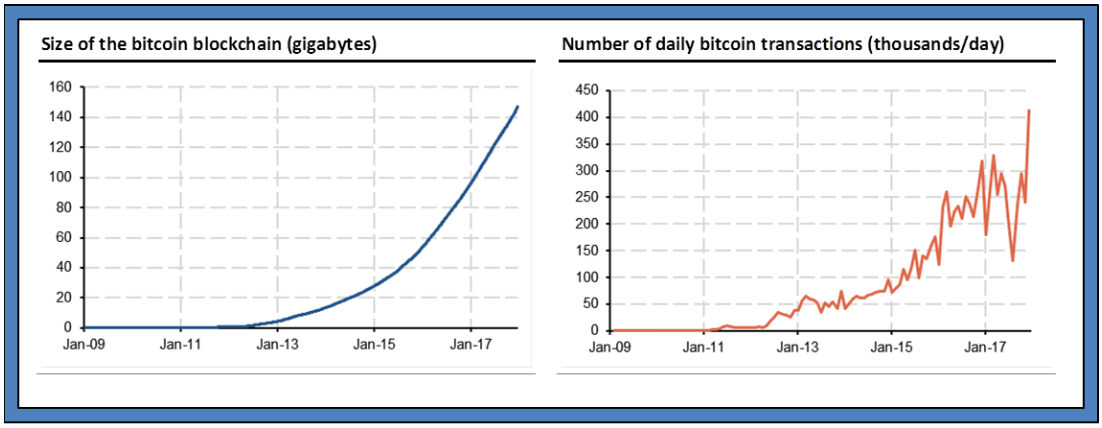
Layer 2: Blockchains

Having introduced hash functions and digital signatures, we can now reintroduce blockchains – the second layer in the bitcoin system. The bitcoin blockchain, like other blockchains, is first and foremost an accounting system, but differ from traditional systems by their decentralized nature.

Blockchains are First and Foremost Accounting Systems

Strictly speaking, a blockchain is a file-like historical record of all past transactions. As for accounting ledgers, entries are sequential, sorted chronologically such that each entry has an antecedent and a descendant. The bitcoin blockchain – that is, the entire history of all bitcoin transactions – can be downloaded as a single file and can fit on most computers. As the number of daily transactions increases, the size of the blockchain will continue to grow as well. Please see Figure 21.

Figure 21



Source: Blockchain.info.

Unlike traditional ledgers however, each entry is uniquely identified by its hash – where the hash is computed from the transaction's characteristics (e.g., sender, receiver, amount…) through the SHA-256 hash function. The hash of a transaction is also a function of the previous transaction's hash.

By way of illustration, we reproduce a simplified blockchain in the below spreadsheet-like figure in Figure 22 on the next page. The spreadsheet (ledger) has five columns, and each transaction is defined by the sender's name (column A), the recipient's name (column B), the transaction amount and signature (column C and D) – and finally its hash (column E). The signature is itself a string of characters and refers to the digital signature generated using the sender's private key.

Figure 22

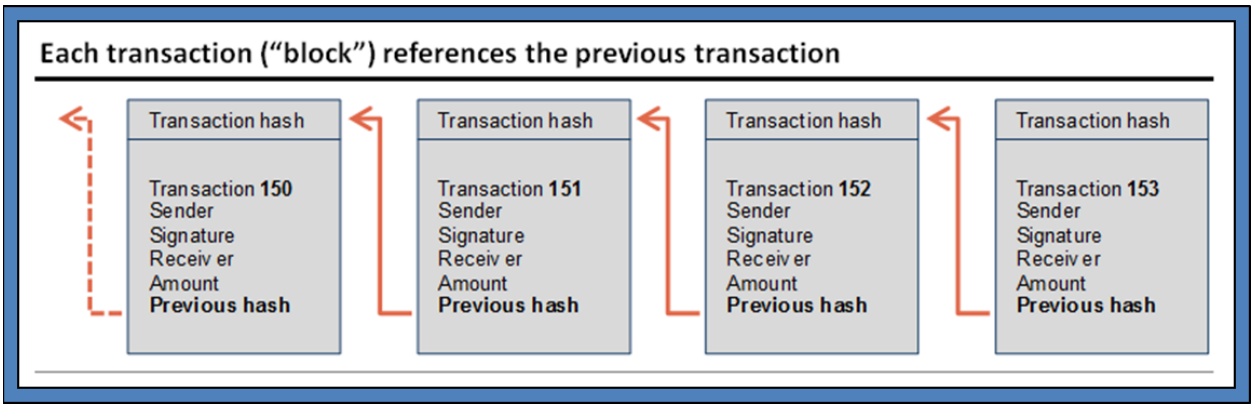
A simplified blockchain implemented in a spreadsheet

	A	B	C	D	E
1	Sender	Receiver	Amount	Signature	Hash
2	David	Nora	10 coins	****	bacbf9c5bf402a8759f577efb49b86d15d65d1a858766612ad15d30268ad2d94
3	Sophie	Mike	20 coins	****	49893f283ea4f2a18b911ef67e1b2535635f5ddfca01573acc74a99132a15c0f
4	Celine	Mark	5 coins	****	=HASH(E3&A4&B4&C4&D4)
5					

Source: SG Cross Asset Research/Commodities.

Importantly, and as noted above, the hash of each transaction (column E) includes the previous transaction's own hash as input. For example, the hash of the third transaction (line 4) is computed using all its features (sender and receiver's name, amount and signature) as well as the hash of the previous transaction on line 3. Likewise, the hash on line 3 refers to the hash on line 2. This way, each transaction iteratively refers the entire history of transactions in its own hash. We illustrate this chaining between blocks in Figure 23 below.

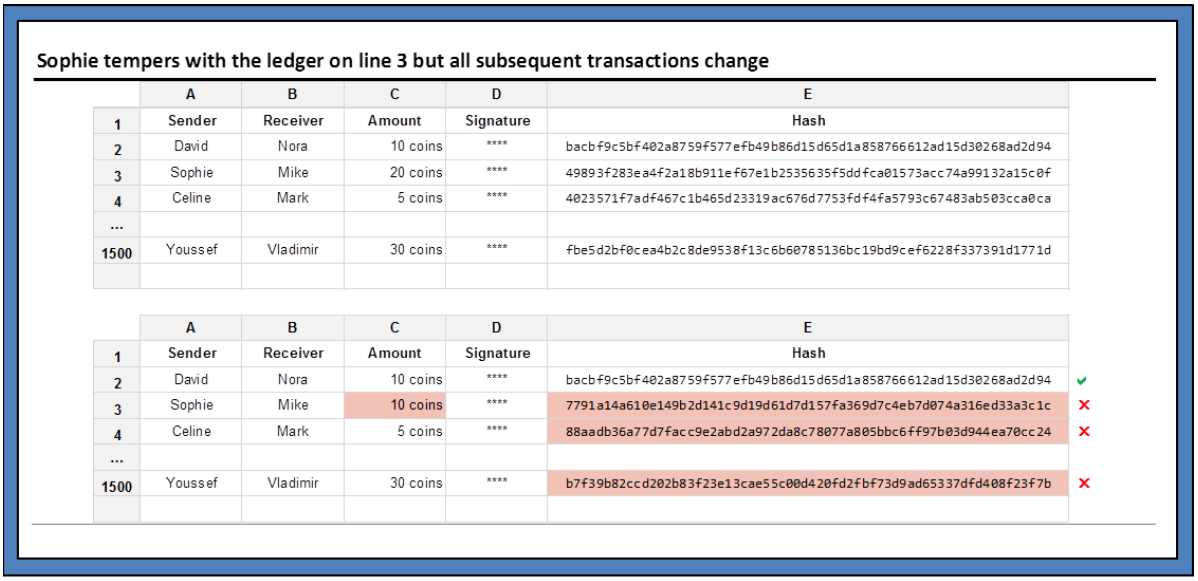
Figure 23



Source: SG Cross Asset Research/Commodities.

The usefulness of including the previous transaction's hash in the subsequent transaction lies with the interdependence created between transactions. Since a transaction's hash acts as a fingerprint, any change to a transaction's content also changes all subsequent transactions. Suppose for instance that a malevolent user – say Sophie – maliciously changed a transaction and claimed to have transferred ten coins rather than original 20. That single change (on line 3 in Figure 24 on the next page) impacts the entire set of subsequent transactions and makes it obvious that an entry has been changed.

Figure 24



Sophie tempers with the ledger on line 3 but all subsequent transactions change

	A	B	C	D	E
1	Sender	Receiver	Amount	Signature	Hash
2	David	Nora	10 coins	****	bacbf9c5bf402a8759f577efb49b86d15d65d1a858766612ad15d30268ad2d94
3	Sophie	Mike	20 coins	****	49893f283ea4f2a18b911ef67e1b2535635f5ddfca01573acc74a99132a15c0f
4	Celine	Mark	5 coins	****	4023571f7adf467c1b465d23319ac676d7753fdf4fa5793c67483ab503cca0ca
...					
1500	Youssef	Vladimir	30 coins	****	fbe5d2bf0cea4b2c8de9538f13c6b60785136bc19bd9cef6228f337391d1771d

	A	B	C	D	E	
1	Sender	Receiver	Amount	Signature	Hash	
2	David	Nora	10 coins	****	bacbf9c5bf402a8759f577efb49b86d15d65d1a858766612ad15d30268ad2d94	✔
3	Sophie	Mike	10 coins	****	7791a14a610e149b2d141c9d19d61d7d157fa369d7c4eb7d074a316ed33a3c1c	✘
4	Celine	Mark	5 coins	****	88aadb36a77d7facc9e2abd2a972da8c78077a805bbc6ff97b03d944ea70cc24	✘
...						
1500	Youssef	Vladimir	30 coins	****	b7f39b82ccd202b83f23e13cae55c00d420fd2fbf73d9ad65337dfd408f23f7b	✘

Source: SG Cross Asset Research/Commodities.

Importantly, the blockchain is a history of transactions rather than a snapshot of account balances. In order to see the balance of an account at a specific moment in time, one instead needs to sum together all the transactions in which that account was involved. The blockchain concept is summarized in Box 2.

Box 2

Summary: blockchains

Blockchains are ledger-like data structures in which each entry makes a reference to the previous entry, regardless of whether these are related. This is a key concept in blockchains, as it underlies the **immutability** of the blockchains: no entry can be tampered with unless all subsequent entries are also amended.

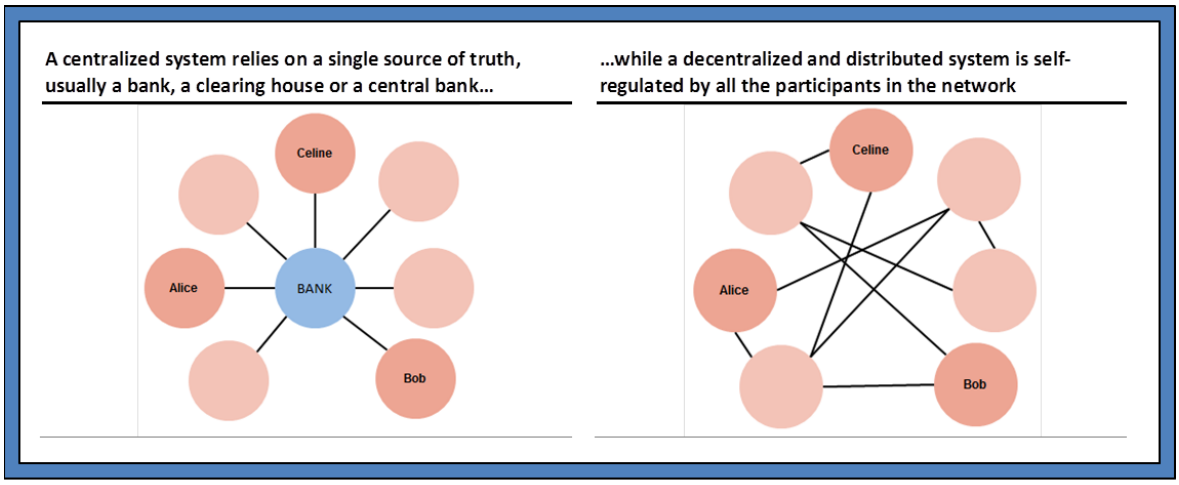
Layer 3: Distribution and Decentralization

The above spreadsheet-like example is still an oversimplified example of a real-life blockchain, but the key difference lies in the centralization of the ledger. Indeed, in the above example, one party maintains and updates the ledger, adding entries over time and the integrity of the entire history hinges on one party. Moreover, the above example does not address the question of how coins are initially created nor does it explain how transactions are recorded in the final ledger. Finally, and importantly, the above example overlooks the fact that blockchain tokens (e.g., bitcoins) ultimately acquire monetary value through a process known as bootstrapping.[3]

In this section, therefore, we show how blockchains like bitcoin solve these problems through an elegant combination of cryptography and game theory. In practice, no single-party controls the ledger, and

many copies of the ledger are simultaneously and competitively updated by a network of participants known as miners. As shown in the illustration in Figure 25, modern blockchains, unlike traditional ledgers, are distributed systems, and there is no centralized source of truth (i.e., ledger.) Instead, the source of truth is determined through a reconciliation process known as consensus. Finally, to ensure the ledger's immutability (and irreversibility of transactions), large amounts of computing power are required to amend the ledger in a process known as mining. We address each of these areas below.

Figure 25



Source: SG Cross Asset Research/Commodities.

The Challenges of Decentralization

Aspects of decentralization percolate through modern blockchains at different levels in the architecture: as briefly stated above, identity management is fully decentralized on the bitcoin blockchain through the self-generation of public-private keys. Furthermore, all participants ("nodes") on the network can, at any time, replicate a copy of the history of transactions and verify its integrity. Participants can furthermore append to the blockchain through a competitive process known as mining, which we explain below.

The key challenge for decentralized systems like blockchains is to achieve consensus – a state in which the majority of participants agree on the value of their shared resource (e.g., which transactions have been validated.) The way in which the network of participants achieves consensus is known as the protocol. The protocol is a set of rules to which participants agree to abide. Theory and practice suggest consensus for decentralized systems is hard to achieve for a number of reasons: for example, some participants in the network may be unable to voice their opinion, others may have malicious intentions and others still may be outright unaware of the proposed change. We refer interested readers to Box 3 on the next page for an example.

Box 3

Two Generals' paradox

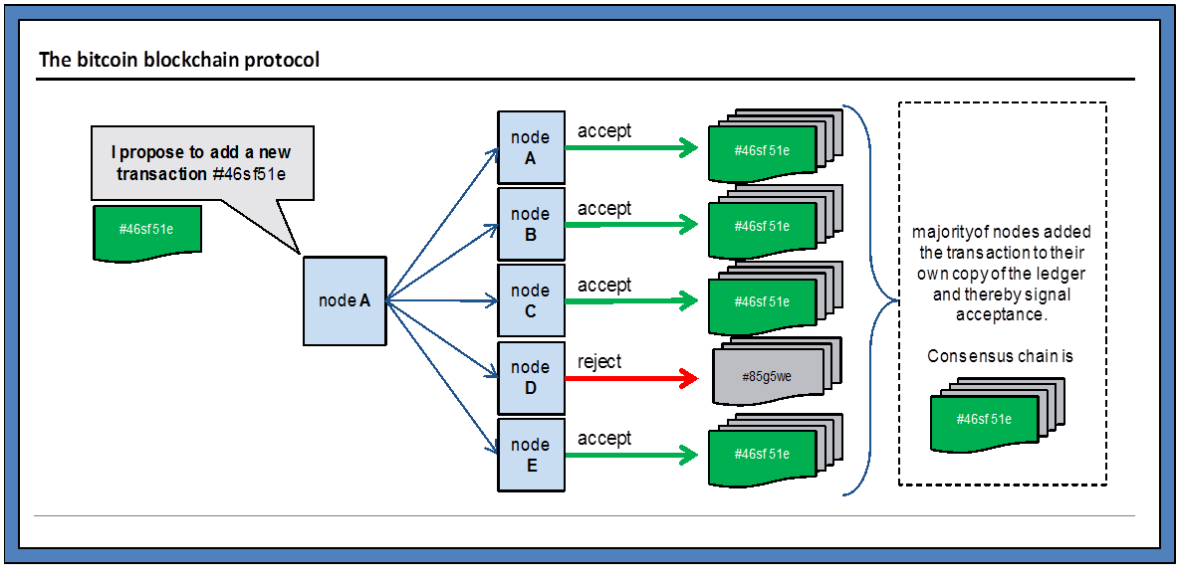
In computer and information science, the difficulty with which a network of participants achieves consensus can be illustrated through a thought-experiment famously known as the *Two Generals' paradox*: two armies, each led by a different general, are preparing to attack a city. For the attack to succeed, both armies must attack simultaneously, or else the lone attacker will be defeated and killed. They must therefore communicate and agree on a time ("consensus"), but importantly, each general must know that the other knows for the attack to succeed. If General A sends General B instructions to attack, he may doubt the latter received the instructions. While General B may send confirmation of the instructions, he in turn may doubt the other general ever received this confirmation – and so forth. A potentially infinite number of messages are required to achieve consensus.

The Rules of the Game: Distributed Consensus

Bitcoin's protocol – its set of rules – is designed such that, at each stage, an active node earns the right to propose adding new transactions it has heard of to the blockchain. Other active participants in the network examine this proposal and verify the transaction's validity – including the sender's signature and the ownership of the tokens being transferred. Each participant individually signals acceptance or rejection of the newly proposed transaction by adding it (or not) to its own copy of the ledger: the network has reached a new consensus.

For example, suppose Mark wanted to send Sophie bitcoins he owned. Mark (node A in Figure 26 on the next page) proposes this new transaction to the network. All other nodes examine the proposal and verify the authenticity of the transaction's signature as well as the existence of the bitcoins Mark claims to own. The participants then accept or reject the transaction by either adding it or not to their own copy of the blockchain. When the majority of the other participants add (or refuse to add) the transaction to their version of the blockchain, then we say the network has achieved consensus. The length of the blockchain increases by one transaction. And as such, the longest observable chain, shared by the majority of nodes, becomes the consensus blockchain.

Figure 26

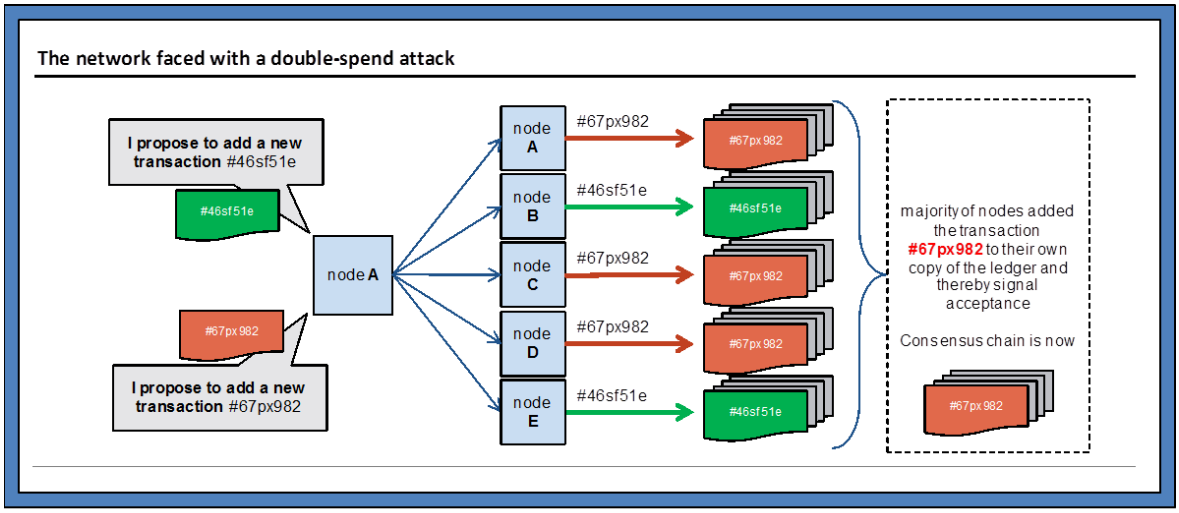


Source: SG Cross Asset Research/Commodities.

Suppose now Mark broadcasts another transaction simultaneously, claiming to send the same bitcoins he sent Sophie to someone else. This is known as the double-spend attack. From the point of view of other participants, both transactions are valid as both have valid signatures and proven funds. And because nodes do not know which transaction came first chronologically, nor which one is supposedly accurate, there is really no way for the network to discriminate among transactions. Instead, each node treats the first proposal they hear about as the only transaction they need to examine. And when the majority of nodes elects to keep one transaction rather than another, that transaction is entered into the consensus chain and the other one is discarded.

For example, node A in Figure 27 on the next page simultaneously proposes two transactions (red and green), both of which claim to transfer the same funds. Nodes A, C and D decide to accept the former, while B and E accept the latter. The consensus chain arbitrarily accepts the red transaction and discards the green. Any subsequent attempt to add the green transaction would now fail, as the proposed transaction's validity would no longer hold (Mark can no longer claim ownership of the funds.)

Figure 27

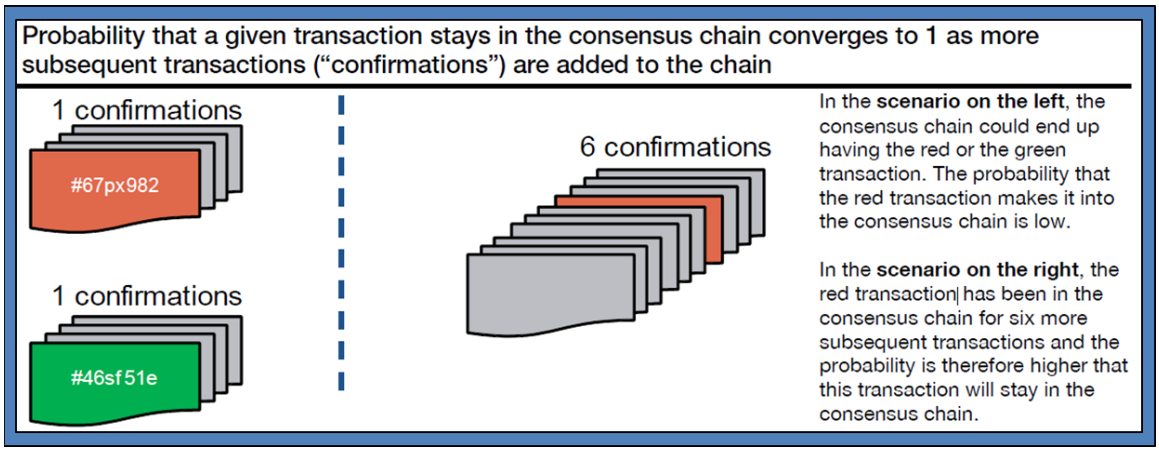


Source: SG Cross Asset Research/Commodities.

In practice, participants group transactions together in bundles known as blocks (hence blockchain.) Each block contains several thousand transactions – but for the purpose of this paper, we will continue to assume that each block contains only one transaction.

In the absence of a central organization, two or more versions of the blockchain may exist side-by-side for a while, but the protocol nevertheless incentivizes nodes to accept the longest valid chain and to discard other valid but shorter versions of the blockchain. As such, as time progresses, participants will accept the biggest blockchain as the ultimate true blockchain. As more entries are added after a given transaction, the probability that the transaction does not remain in the consensus chain therefore diminishes exponentially over time; please see Figure 28.

Figure 28

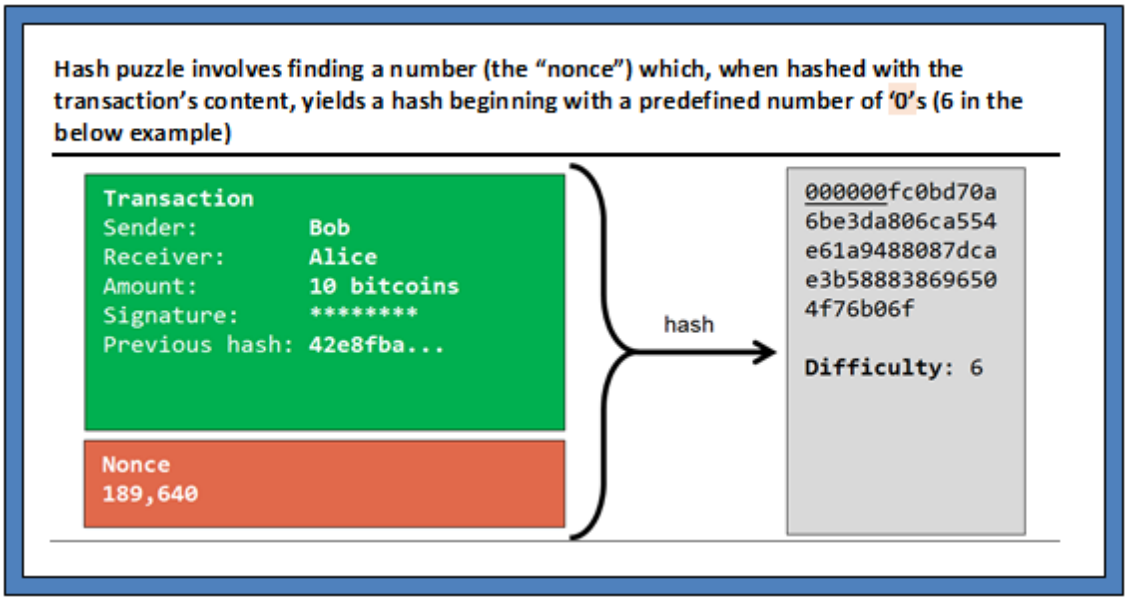


Source: SG Cross Asset Research/Commodities.

Earning your Rights: Proof-of-Work (POW)

We stated above that an active node earns the right to propose adding a new transaction it has heard of to the blockchain. The process through which a node earns this right is known as mining. Mining involves finding a number, called the nonce, which solves a very difficult cryptographic puzzle, the solution to which can only be found by trying a very large number of random values. Specifically, the puzzle involves finding a number, which, when hashed with the transaction's content (sender, receiver…), yields a hash beginning with a predefined number of '0's.[4]

Figure 29



Source: SG Cross Asset Research/Commodities.

For example, suppose Mark, a participant on the network, heard of the above transaction (in green), involving a transfer of ten bitcoins from Bob to Alice. Also, assume that the difficulty is set to 6. As illustrated in Figure 29 above:

1. Mark would first verify the integrity of the transaction by checking if Bob indeed has ten bitcoins to spend.

2. Mark would also check the authenticity of the transaction by verifying the signature.

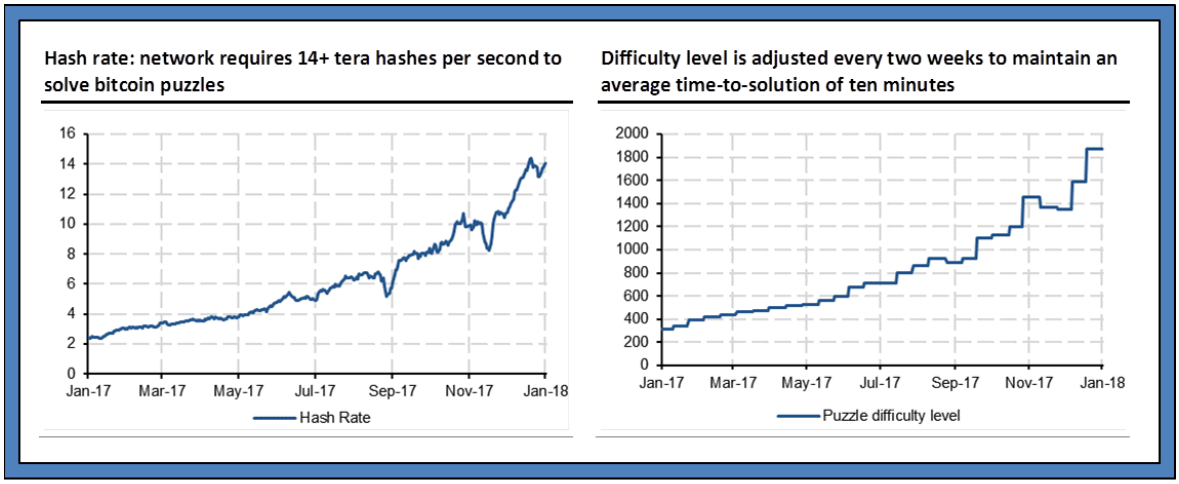
3. Mark then iteratively tries random numbers (1, 2, 3… 189,640) until he finds one which, when hashed together with the transaction's content, yield a hash which begins with at least six '0's.

In the above example, a solution to the problem is 189,640: the hash of the transaction's hash along with that number produces a new hash starting with 000000fc…, which indeed begins with six zeroes. This is only one of many solutions: 6,591,810 is also a solution, for example.

Having solved this puzzle, Mark can now broadcast the transaction along with his solution to the rest of the network. Other participants on the network can verify the transaction as well as Mark's proposed solution, and if the proposed transaction indeed reconciles, they can then update their personal copy of the blockchain using the normal protocol.

Solving the above example is simple and takes less than a minute using a standard computer. In practice, the difficulty is significantly higher, and is adjusted every two weeks such that, on average, a solution is found every ten minutes by the bitcoin network. As of the writing of this article, the network requires the final hash to begin with at least 18 '0's, implying miners must currently try 14 million trillion hashes per second (14,000,000,000,000,000,000,000/second). Please see Figure 30.

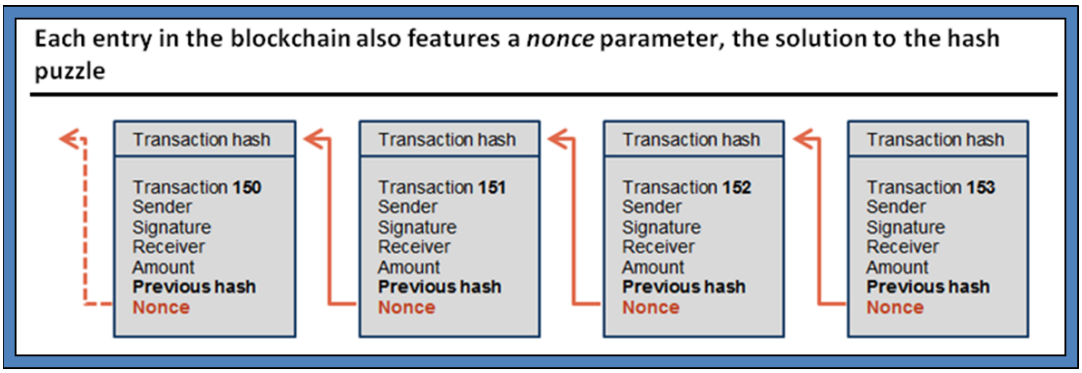
Figure 30



Source: SG Cross Asset Research/Commodities.

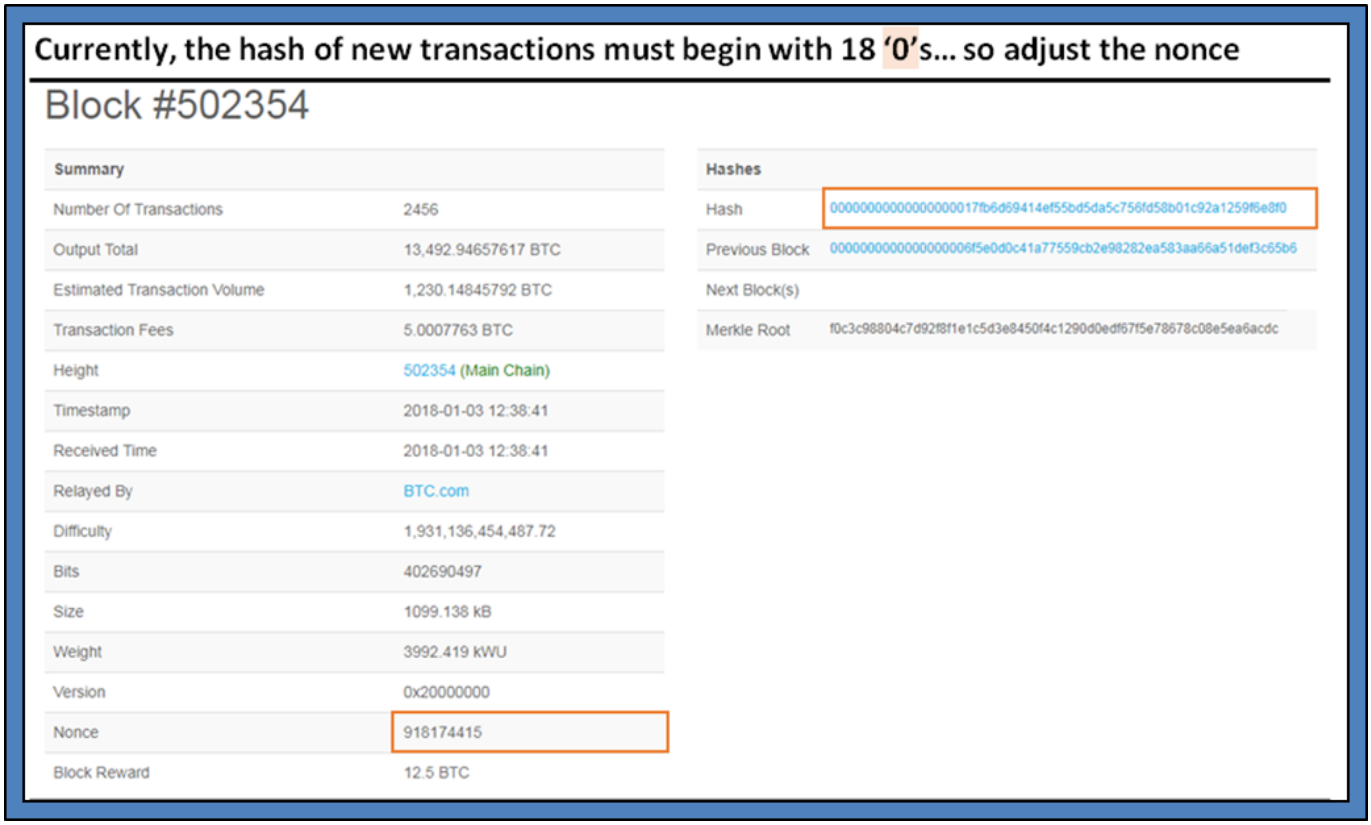
Each record on the bitcoin blockchain therefore also contains the solution of the hash puzzle, and is required to record the transaction on the blockchain. Please see Figure 31 (below) and Figure 32 (on the next page.)

Figure 31



Source: SG Cross Asset Research/Commodities.

Figure 32



Source: SG Cross Asset Research/Commodities, blockchain.info.

The difficulty of finding the solution to a hash puzzle underpins the immutability of the blockchain. If one wanted to temper – or reverse – a past transaction, one would not only need to solve the puzzle of the affected transaction, but also of all subsequent transactions to create a blockchain longer than what other participants currently have. And, as the number of participants increase, the probability of controlling enough computing power to outpace the network falls to zero. In the word of bitcoin's author, Satoshi Nakamoto:

> The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.

Obviously, solving hash puzzles involves deploying lots of computing power and electricity – and the bitcoin protocol features clever incentives to encourage participants to become involved in this costly process, colloquially known as mining. Indeed, in order to incentivize participants to solve these hash puzzles, the blockchain rewards the miner with a number of bitcoins (currently 12.5 per block of transactions for each hash puzzle they solve.) This reward is created *ex-nihilo*, and is the source of any bitcoin in circulation: stated differently, all bitcoins in circulation were, at one point in time, a reward

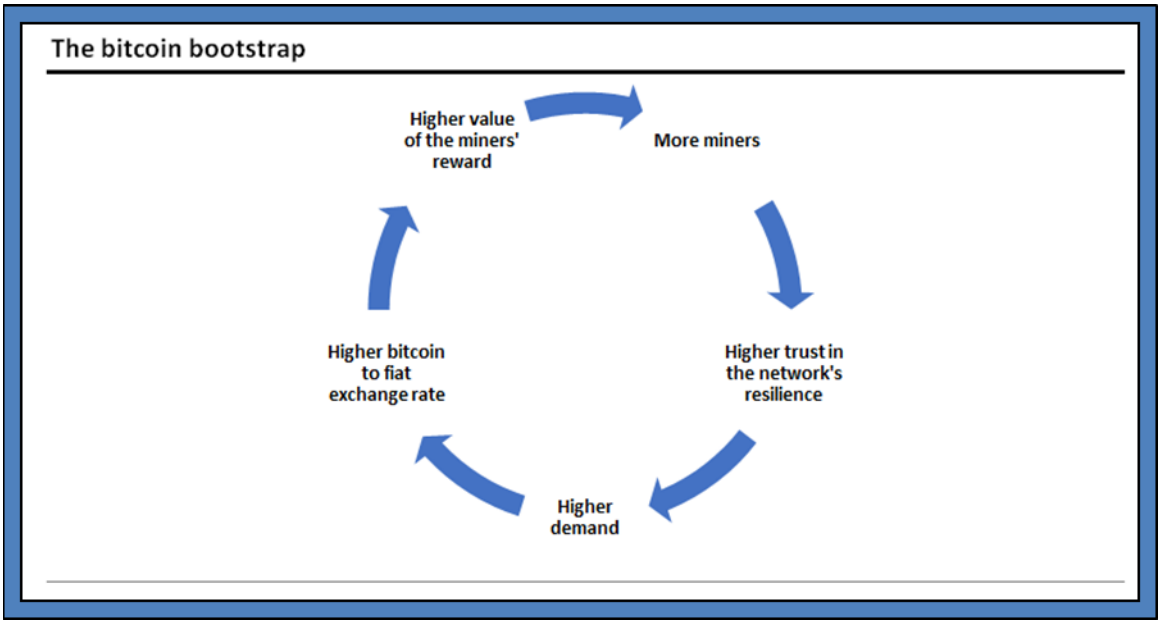
attributed to a miner. But importantly, the reward is only valuable on the longest blockchain, therefore incentivizing participants to accept the longest chain as the source of truth.

Layer 4: Putting Everything Together – Bootstrapping Bitcoin

Convertibility into fiat currencies is the last crucial element of the system. While miners are rewarded with bitcoins, their electricity and computing costs are however in fiat currencies (e.g., USD, CNY…), and allowing these participants to convert the former into the latter is a key imperative for a healthy mining ecosystem.

Bootstrapping refers to the mutual dependence between demand for bitcoins, mining profitability and trust in the system. Please see Figure 33. As more miners compete to maintain the blockchain, the probability that a transaction can be reversed falls. Therefore, trust in the system's ability to confirm transactions rises. As trust increases in bitcoin, so will demand, which will push the exchange rate higher. And finally, a higher exchange rate makes mining more profitable, hence more attractive.

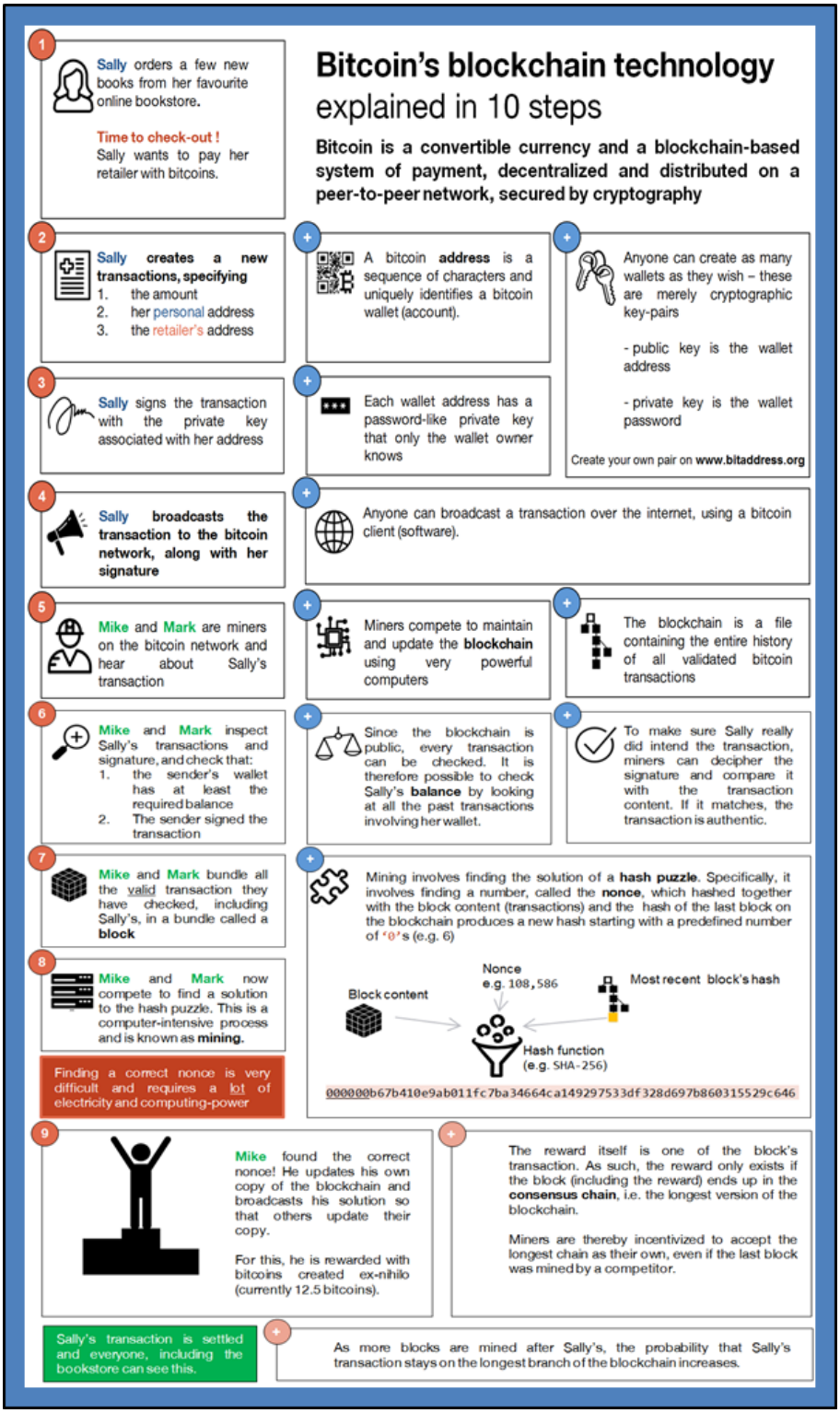
Figure 33



Source: SG Cross Asset Research/Commodities.

In summary, Figure 34 on the next page explains bitcoin's blockchain technology in ten steps.

Figure 34



Note: Icons courtesy of the "Noun Project." Please see the endnotes for attributions.

Source: SG Cross Asset Research/Commodities.

Conclusion

Bitcoin and the underlying blockchain technology are still in their early days. Within the cryptocurrencies space, Bitcoin could be viewed as a proof of concept. The blockchain has demonstrated the feasibility of decentralization and opened the way for many more applications. It is also starting to show its limits. The cost of mining, during which transactions are validated and then recorded on the blockchain, has recently exploded, both in monetary and electricity terms. Other blockchains are already moving to less energy-hungry models.

In this paper, we have tried to address many of the questions about this nascent technology. We stress that the piece is solely an educational piece – we express no opinion, view or endorsement of cryptocurrencies, bitcoin or the blockchain technology.

Endnotes

1 Tokens are a representation of a particular asset or utility, whereas a coin is in and of itself the asset. For example, a government could use a token blockchain to manage its land registry.

2 Tokens can be used with smart-contracts, which allow for the automatic transfer of ownership contingent on a trigger (e.g., weather.)

3 This is a distinct concept from statistical bootstrapping.

4 Technically, hashes are base-16 numbers, and solving the hash puzzle involves finding a hash smaller than a specified threshold.

*Icon Attributions: Woman by Gregor Cresnar from the Noun Project; medical form by Royyan Wijaya from the Noun Project; Bitcoin Address by useiconic.com from the Noun Project; house keys by b farias from the Noun Project; autograph by Royyan Wijaya from the Noun Project; OTP by Ayushi Bhandari from the Noun Project; internet by Asimbla from the Noun Project; miner by ProSymbols from the Noun Project; CPU by Aiden Icons from the Noun Project; Blockchain by Jason D. Rowley from the Noun Project; Zoom In by Weltenraser from the Noun Project; Puzzle by IconDots from the Noun Project; Funnel by Gregor Cresnar from the Noun Project; Shared Hosting by b farias from the Noun Project; winner by Hopkins from the Noun Project.

This article is a republication of Société Générale Cross Asset Research, *Commodity Compass*, January 10, 2018.

Author Biographies

MARK KEENAN
Managing Director, Global Commodities Strategist and Head of Research for Asia-Pacific, Société Générale Corporate & Investment Bank (Singapore); and Editorial Advisory Board Member, *Global Commodities Applied Research Digest*

Mr. Mark Keenan is the Global Commodities Strategist and Head of Research for Asia-Pacific (Managing Director) at Société Générale Corporate & Investment Bank in Singapore. He is also the author of Positioning Analysis in Commodity Markets (2018). With over 20 years of research, trading and investment experience across all the major energy, metal, agriculture and bulk commodity markets, Mr. Keenan works with corporates, trade houses, investment institutions and hedge funds to develop better trading, hedging and investment solutions. Specific expertise in modelling supply and demand data, combined with sentiment, uncertainty, flow and positioning analysis helps him understand commodity price behavior and how it responds to changes in currencies and a variety of different macroeconomic variables. Mr. Keenan has worked in asset management, risk management and investment banking in both London and Singapore. He appears regularly on CNBC and Bloomberg television and is quoted widely in global press and media channels. He has a B.A. and M.A. in Molecular and Cellular Biochemistry from Oxford University.

MICHAEL HAIGH, Ph.D.
Managing Director and Global Head of Commodities Research, Société Générale (U.S.)

Dr. Michael Haigh is Managing Director and Global Head of Commodities Research for Société Générale and is based in NYC. For 2017, 2016, 2015, 2014 and 2013, SG CIB has been voted by the industry as the Best Overall in Commodity Research in both *Risk* and *Energy Risk*, two highly respected publications dedicated to risk management, trading and regulation for the global commodity markets. Immediately prior to running the Global Commodities Research team, Dr. Haigh was Global Head of Commodities Research at Standard Chartered Bank, based in Singapore. Prior to joining Standard Chartered Bank, Dr. Haigh held the positions of Managing Director at K2 Advisors LLC, a Global Hedge Fund of Funds where he focused on Commodity Research/Investing and also as Managing Director and U.S. Head of Commodities Research and Strategy at Société Générale in NYC. Dr. Haigh also spent several years as the Associate Chief Economist at the U.S. Commodity Futures Trading Commission (CFTC). He began his career in academia and held a position as a tenured Associate Professor of Economics at the University of Maryland, U.S. Dr. Haigh has taught graduate (M.B.A.) & undergraduate derivative courses at several universities including NYU Stern School of Business, Johns Hopkins University and George Washington University and has supervised numerous Ph.D. dissertations on the commodity and financial markets. He has published numerous scholarly research papers on commodity and derivative markets in several leading journals including the *Journal of Finance*, *Journal of Business*, *Journal of Futures Markets*, and the *Journal of Applied Econometrics*. Dr. Haigh holds a Ph.D. in Economics with a minor in Statistics from North Carolina State University.

DAVID SCHENCK
Commodities Analyst, Société Générale (U.K.)

Mr. David Schenck is a Commodities Analyst based in London. He joined Société Générale in 2016. Mr. Schenk holds a Master's degree in International Finance from HEC Paris (France) and a Bachelor's degree in Economics from Trinity College Dublin (Ireland).

KLAUS BAADER
Global Chief Economist, Société Générale (U.K.)

Mr. Klaus Baader is Global Chief Economist for Société Générale and based in London. Before relocating to London in 2018, he was Chief Economist Asia Pacific, based in Hong Kong, and prior to that, Chief Euro Area Economist in London. He joined Société Générale in July 2009 from Merrill Lynch where he had been Chief Europe Economist since 2006. Previously, he was at Lehman Brothers for 10 years, latterly as Senior Europe Economist. He has also held positions at UBS and Deutsche Bank. Mr. Baader began his career at Salomon Brothers in 1989 after studying Economics and Political Science at the University of Cologne and the London School of Economics. He received his B.Sc. in Economics from the LSE in 1988 and completed his Master's in Economics in 1989.